REMARKS

In response to the Official Action dated 7/25/2005, the applicants provide the following remarks.

It appears that in reviewing the Office Action, it is unclear whether the Examiner reviewed the amended claims per the Supplemental Amendment filed on 5-31-2005 (copy of which is included herewith along with an auto reply fax transmission copy). A copy of the PAIR herewith shows that the Supplemental Amendment was not entered.

It is respectfully submitted that it may be premature for Applicants to respond to the above-identified Office Action until receiving an Office Action which addresses the claims as previously amended. Accordingly, since Applicants are unaware of what references the examiner may rely upon in responding to said prior Supplemental Amendment, Applicants reserve responding in full to the current and future rejections.

In any event, Applicants will attempt to address the basis of the rejections. The Examiner rejected claims 1-7, 9-16 and 18 under 35 U.S.C.§ 103 as unpatentable over Johnson et al. in view of Dillon. The examiner stated that all the elements are found in Johnson save for the initiating a registration authorization process and monitoring process.

The applicants respectfully traverse. Claim 1 calls for:

A method for synchronizing databases among a server computer having a master database therein, and a client computer in communication with the server computer, wherein the client computer having a replica database of the master database therein, comprising the steps of:

establishing communication between a server computer having a master database therein

and a client computer;

recognizing a replication request by said client computer for a piece of data within said master database from said server computer, wherein said server computer initiates a secure session using an authentication session;

initiating a registration authorization process of said client computer wherein said client computer is provided with means for accessing multicast updates of said data, wherein said accessing means includes a multicast address and encryption key;

a monitoring process on said server computer that recognizes when an update is made to said master database on said server computer and then multicasting said update to said client computer using said multicast address and encryption key; and

accessing a multicast of updated data using said accessing means.

Johnson is simply an invention directed to method of broadcasting data to a plurality of other nodes using a two stage multicast. The invention describes using a multicast broadcast first to send the data, where if unsuccessful, a point to point transmission is subsequently performed to transmit the data. Johnson states point-to-point communications are not well suited for multicast message transmissions – particularly in systems with large number of nodes (col. 4, lines 37-41) as the resources are overly burdened. Johnson employs a paradigm which sends a multicast which uses an acknowledgement receipt from the recipient to determine whether the data is received. If not, the multicast sender will begin sending the multicast message point to point to those nodes not providing an acknowledgement (col.7, lines 9-22). This was thought to save resources.

Johnson is the typical multicast approach which applicants discussed in the present invention. Johnson describes the mechanics of how it transmits information using a multicast

paradigm.

Dillon relates to a system for multicasting multimedia. Dillon is concerned with the broadcast of media channels using a multicast paradigm. If a client wants a particular media show, Dillon provides a mechanism whereby the content viewer contacts the registration server of the back end subsystem and performs a subscribe transaction. The transaction request includes information: (i) identifying the multicast receiver that the receiver is receiving from, (ii) the channel being requested, and (iii) optionally, information used to authenticate the sender of the request. This enables the viewer to receive the channel, such as the Disney channel. As the Examiner points out, the authentication is intended to verify that the request came from the content viewer of the receiver for which access to a channel is being requested. Johnson states that the authentication is preferably performed via password authentication, however, authentication may also be performed using public key encryption.

This citing of Dillon appears misplaced. Dillon is concerned with transmitting media channels to a viewer, not the synchronization of data objects within and between databases in a secure network environment as with the instant invention. Neither reference provides a monitoring process on the server computer that recognizes when an update is made to the master database on the server computer and then multicasting the update to the client computer using the multicast address and encryption key as in the present invention. Rather, Dillon simply periodically transmits updated media content. This may work fine for primarily receive only applications in the case of media, but falls inadequate in scenarios as the present invention contemplated in which the nodes may be presenting and receiving changes to the database or replication quests and the server computer monitors such changes and initiates a broadcast of

such changes real time.

It is respectfully submitted that it would not have been obvious to incorporate the teaching of Dillon into Johnson. Johnson uses multicasting on a periodic basis with continual multicasting of for non-responsive nodes until the updates are received by the nodes. Dillon provides for periodic multicasting and although mentions a secure way to enable users to receive such multicasts, this would have provided no advantage to Johnson. Similarly, Dillon was not concerned with synching databases in a secure network real time between users so he would not have looked to Johnson. Even if the references were combined, there is no teaching, suggestion or disclosure for monitoring process on the server computer that recognizes when an update is made to the master database on the server computer and then multicasting the update to the client computer using the multicast address and encryption key.

Further, Johnson's multicast permits any member to go to a multicast and obtain the information for purposes of resynchronization. This is not so with the instant invention. There first must be an authentication session, wherein an open subscription request is made. Then, there must be a multicast address and encryption key delivered to the client computer in order to obtain the multicast data. Johnson does not provide any teaching, suggestion or disclosure of a method or system which "recognizes a replication request by the client computer for a piece of data within the master database from the server computer, wherein the server computer initiates a secure session using an authentication session and initiating a registration authorization process of the client computer wherein the client computer is provided with means for accessing multicast updates of the data, wherein the accessing means includes a multicast address and encryption key.

Claims 1-19 are respectfully submitted to be patentably distinct over the art. Withdrawal

of the rejection is respectfully requested of claims 1-19 is requested.

Claims 8, 17 and 19 were further rejected under 35 U.S.C. 103(a) over Johnson in view of Bhagavath. It was stated that Bhagavath disclosed a multicast approach and the technique of encrypting data. Bhagavath discloses a system for repairing missed packets in a multicast transmission using encryption/decryption techniques.

In the present invention, it is not simply the concept of multicasting of data which is being claimed in the invention nor the encryption of data during a transmission. The instant invention teaches a unique method of securely integrating multicasting of database updates as they occur inside a system where a security paradigm and replication mechanism already exists. The present invention gracefully integrates with the existing replication systems without introducing new operational methods to the replication process. This is accomplished by providing server software which recognizes a replication request by the client computer for a piece of data within the master database from the server computer, wherein the server computer initiates a secure session with the client computer using an authentication session and initiating a registration authorization process of the client computer wherein the client computer is provided with means for accessing multicast updates of the data, wherein the accessing means includes a multicast address and encryption key. This is not taught, suggested or disclosed by the art nor would it be obvious.

The invention is not obvious and is patentably distinct over the art. None of art describes such a method or a system which in effect plugs into a database replication system and securely transmits updates within the existing paradigm of the database real time and this is what is accomplished through the instant invention.

Accordingly, withdrawal of the rejection is respectfully requested and allowance of claims 1-19 is requested at as early a date as possible. This is intended to be complete response to the Official Action dated 7/25/2005

Respectfully submitted,

R. William Graham, 33891

Certificate of Transmission

I hereby certify that this correspondence is being faxed to the PTO fax number 571 273 8300 for group 2155 on the date shown below.

Date. October 25, 2005 R. William Graham, 33,891

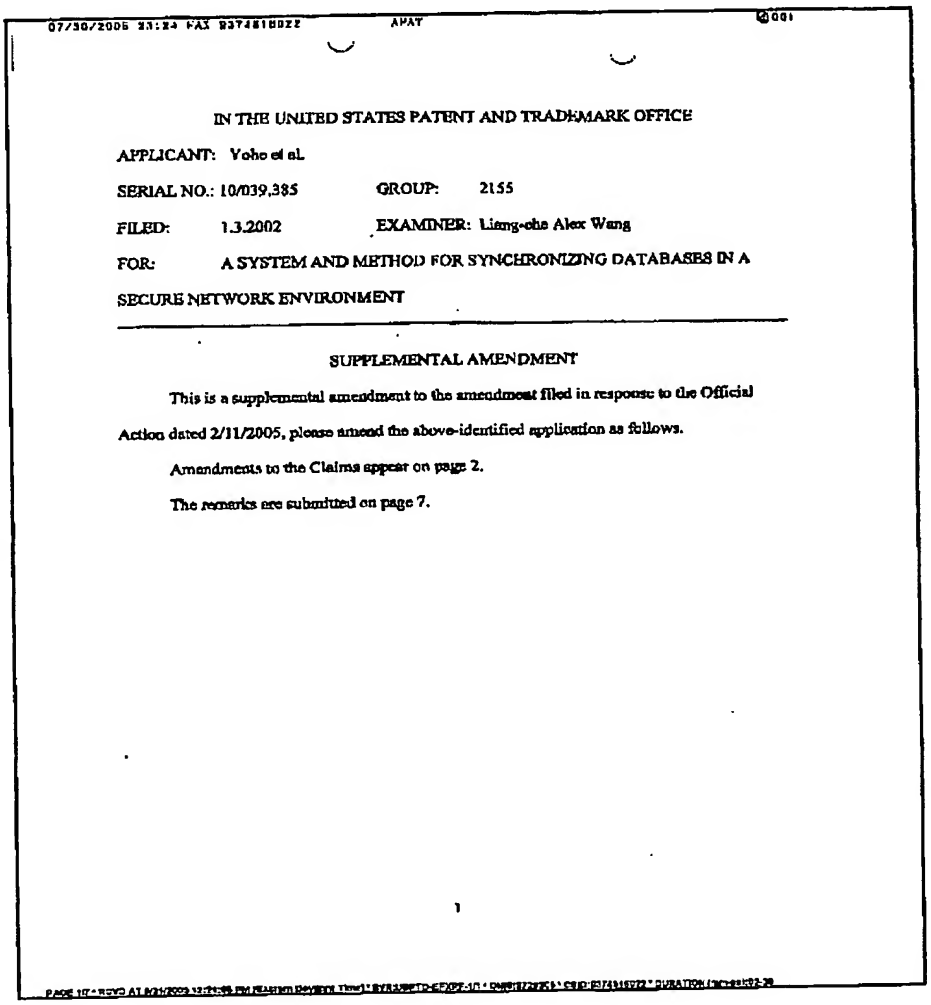
Auto-Reply Facsimile Transmission

TO: Fax Sender at 9374616922

Fax Information
Date Received: 5/31/2005 12:21:06 PM [Eastern Daylight Time]
Total Pages: 7 (Including cover page)

ADVISORY: This is an automatically generated return receipt confirmation of the facsimile transmission received by the Office. Please check to make sure that the number of pages listed as received in Total Pages above matches what was intended to be sent. Applicants are advised to retain this receipt in the unlikely event that proof of this facsimile transmission is necessary. Applicants are also advised to use the certificate of facsimile transmission procedures set forth in 37 CFR 1.8(a) and (b), 37 CFR 1.6(f). Trademark Applicants, also see the Trademark Manual of Examining Procedure (TMEP) section 306 et seq.

Received Cover Page ========>



05/31/2005 12:24 FAX 9374616922 APAT 001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Yoho et al.

SERIAL NO.: 10/039,385 GROUP: 2155

FILED: 1.3.2002 EXAMINER: Liang-chu Alex Wang

FOR: A SYSTEM AND METHOD FOR SYNCHRONIZING DATABASES IN A SECURE NETWORK ENVIRONMENT

SUPPLEMENTAL AMENDMENT

This is a supplemental amendment to the amendment filed in response to the Official Action dated 2/11/2005, please amend the above-identified application as follows.

Amendments to the Claims appear on page 2.

The remarks are submitted on page 7.

1

RECEIVED
CENTRAL FAX CENTER
OCT 25 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Yohe et al.

SERIAL NO.: 10/039,385 GROUP: 2155

FILED: 1.3.2002 EXAMINER: Liang-che Alex Wang

FOR: A SYSTEM AND METHOD FOR SYNCHRONIZING DATABASES IN A SECURE NETWORK ENVIRONMENT

SUPPLEMENTAL AMENDMENT

This is a supplemental amendment to the amendment filed in response to the Official Action dated 2/11/2005, please amend the above-identified application as follows.

Amendments to the Claims appear on page 2.

The remarks are submitted on page 7.

Listing of Claims.

1. (currently amended) A method for synchronizing databases among a server computer having a master database therein, and a client computer in communication with the server computer, wherein the client computer having a replica database of the master database therein, comprising the steps of:

establishing communication between a server computer having a master database therein and a client computer;

recognizing a replication request by said client computer for a piece of data within said master database from said server computer, wherein said server computer initiates a secure session using an authentication session;

initiating a registration authorization process of said client computer wherein said client computer is provided with means for accessing multicast updates of said data, wherein said accessing means includes a multicast address and encryption key;

a monitoring process on said server computer that recognizes when an update is made to said master database on said server computer and then multicasting said update out to said client computer using said multicast address and encryption key; and

accessing a multicast of updated data using said accessing means.

2. (previously presented) The method of claim 1, which is further includes the steps of determining a missed multicast of updated data by said client computer and initiating a unicast of said missed updated data.

3. (previously presented) The method of claim 1, which is further characterized as:

establishing a connection between said server computer and a plurality of client

computers;

recognizing a replication request by each said client computer for a piece of data within said master database from said server computer;

initiating a registration authorization process of said client computers wherein said client computers are provided with means for accessing multicast updates of said data; and

accessing a multicast of updated data using said accessing means.

4. (previously presented)The method of claim 3, wherein said step of recognizing replication requests are for different data for each said client computer.

5. (previously presented) The method of claim 1, which further includes the step of determining whether to receive said update of said data.

6. (previously presented) The method of claim 5, wherein the step of determining is accomplished by maintaining in said client computer information relating to prior updates of said data by said client computer.

7. (previously presented)The method of claim 5, wherein the step of determining is accomplished by maintaining in said server computer information relating prior updates of said data by said client computer.

8. (previously presented)The method of claim 1, which further includes the step of determining the rate at which to multicast said data between said server computer and said client computer.

9. (previously presented) A system for synchronizing databases among a server computer having a master database therein, and a client computer in communication with the server computer, wherein the client computer having a replica database of the master database therein, comprising:

a server computer having means for storing a master database therein;

a client computer having means for storing a replica of said master database;

means for communicably connecting said server computer to said client computer;

means for recognizing a replication request by said client computer for a piece of data within said master database of said server computer;

means for initiating a registration authorization process of said client computer and providing said client computer with means for accessing multicast updates of said data, wherein said initiating means includes software for initiating a secure session using an authentication session between said client computer and said server computer; and

means for accessing a multicast of updated data using said accessing means, wherein said accessing means includes a multicast address and encryption key.

10. (previously presented) The system of claim 9, which further includes means for determining a missed multicast of prior update of said data by said client computer and means for initiating a unicast of said missed prior update of said data.

11. (previously presented)The system of claim 9, which is further characterized to include:

a plurality of said client computers;

means for establishing a connection between said server computer and said plurality of client computers;

means for recognizing a replication request by each said client computer for a piece of data within said master database from said server computer; and

means for initiating a registration authorization process of said client computers wherein said client computers are provided with means for accessing multicast updates of said data; and

means for accessing a multicast of updated data using said accessing means.

12. (previously presented) The system of claim 11, wherein said data are different for each said client computer, and said means for accessing multicast updates of each said different data are different for each client computer.

13. (previously presented) The system of claim 9, which further includes means for determining whether to receive said update of said data.

14. (previously presented)The system of claim 13, wherein said determining means is accomplished by maintaining in said client computer information relating to prior updates of said data by said client computer.

15. (previously presented)The system of claim 13, wherein said determining means is accomplished by maintaining in said server computer information relating prior updates of said data by said client computer.

16. (previously presented)The system of claim 9, wherein said file server computer has an operating system, a first memory, a permanent storage memory and a processor an object server software which includes an object synchronization server, an object update hook, an object update detector, an object update multicator, a multicast communication protocol, and a unicast communication protocol and an object database, and said client computer has an operating system, a first memory and a processor, an object client computer has a client object requester software which includes an object synchronization client and a multication client, a multicast communication protocol, and a unicast communication protocol, and an object database replica.

17. (previously presented) The system of claim 16, wherein said object server software includes means for encrypting said data and transmitting an encryption key sequence with said data and said client object requester software will include said accessing means which includes means for verifying said encryption key and de-encrypting said data.

18. (previously presented) The system of claim 9, wherein said client computer is equipped to be as a server.

19. (previously presented) The system of claim 9, which further includes means for determining the rate at which to multicast said data.

REMARKS

This is a supplemental amendment in furtherance of the prior amendment in response to the Official Action dated 2/11/2005. Review and reconsideration are requested in view of the above amendments and following remarks.

Applicant has further amended claim 1 to include the step of "a monitoring process on said server computer that recognizes when an update is made to said master database on said server computer and then multicasting said update out to said client computer using said multicast address and encryption key." Applicant reasserts and alleges all prior remarks in the amendment previously filed.

The supplemental amendment is not believed to require any additional fee, however, to the extent such is deemed required, please charge account 500353.

Respectfully submitted,

R. William Graham

Date. 5-31-05

Certificate of Transmission

I hereby certify that this correspondence is being faxed to the PTO fax number 703-872-9306 for group 2155 on the date shown below.

Date. May 31, 2005 R. William Graham

United States Patent and Trademark Office

PATENT APPLICATION INFORMATION RETRIEVAL

Search results as of: 10-25-2005::9:27:36 E.T.

Search results for application number: 10/039,385			
Application Number:	10/039,385	Customer Number:	25179
Filing or 371(c) Date:	01-03-2002	Status:	Final Rejection Mailed
Application Type:	Utility	Status Date:	07-25-2005
Examiner Name:	WANG, LIANG-CHE	Location:	ELECTRONIC
Group Art Unit:	2155	Location Date:	-
Confirmation Number:	2011	Earliest Publication No:	US 2003-0126162 A1
Attorney Docket Number:	S-00014-008	Earliest Publication Date:	07-03-2003
Class/ Sub-Class:	709/203	Patent Number:	-
First Named Inventor:	Thomas Yohe, Dayton, OH (US)	Issue Date of Patent:	-
Title Of Invention:	System and method for synchronizing databases in a secure network environment		

Search Options

- Assignments
- Display References
- Image File Wrapper
- Publication Review
- Published Documents

File History

Date	Contents Description
07-25-2005	Mail Final Rejection (PTOL - 326)
07-22-2005	Final Rejection
06-03-2005	Date Forwarded to Examiner
05-20-2005	Response after Non-Final Action
05-20-2005	Request for Extension of Time - Granted
02-11-2005	Mail Non-Final Rejection
02-07-2005	Non-Final Rejection
02-03-2005	Case Docketed to Examiner in GAU
12-23-2004	IFW TSS Processing by Tech Center Complete
01-03-2002	Reference capture on IDS
07-21-2003	Case Docketed to Examiner in GAU
08-25-2002	Receipt of all Acknowledgement Letters

01-03-2002	Information Disclosure Statement (IDS) Filed
07-02-2002	Case Docketed to Examiner in GAU
02-15-2002	Application Dispatched from OIPE
02-14-2002	Application is Now Complete
02-07-2002	Referred by L&R for Third-Level Security Review. Agency Referral Letter Generated
02-06-2002	IFW Scan & PACR Auto Security Review
01-18-2002	IFW Scan & PACR Auto Security Review
01-03-2002	Initial Exam Team nn